Cyberbezpieczeństwo fundamentem nowoczesnej suwerenności państwa

Piotr Mieczkowski
Członek Zarządu, KIGEiT

Cyberbezpieczeństwo nie jest już tylko domeną informatyków – to fundament nowoczesnej suwerenności państwa. W dobie geopolitycznych napięć, wojny informacyjnej i cyfrowej inwigilacji, Polska musi zbudować własną – odporną i niezależną – infrastrukturę cyfrową. Kluczem są inwestycje w krajowy sektor ICT, rozwój kompetencji strategicznych, a także ścisła współpraca z partnerami europejskimi w oparciu o wspólne wartości i standardy technologiczne.

Współczesne gospodarki coraz mocniej opierają się na cyfrowych fundamentach – bez technologii informatycznych i niezawodnej infrastruktury sieciowej nie sposób dziś mówić ani o rozwoju, ani o elementarnym funkcjonowaniu państwa. Zapewnienie cyberbezpieczeństwa stało się zatem warunkiem niezbędnym do zachowania stabilności działania kraju – jego brak może oznaczać paraliż podstawowych funkcji życia społeczno-gospodarczego. Wystarczy wyobrazić sobie *blackout* energetyczny wywołany atakiem hakerskim: systemy płatności elektronicznych przestają działać, sklepy zostają zamknięte, łańcuchy dostaw załamują się, a komunikacja zamiera. Scenariusze, które niegdyś przypominały *science fiction* – znane choćby z seriali „*Zero Day*" czy niemieckiego „*Blackout*" – dziś stają się coraz bardziej realne. Wystarczy wspomnieć atak Stuxnet na elektrownię jądrową czy rosnącą liczbę operacji wywiadowczych prowadzonych w cyberprzestrzeni. Cyberbezpieczeństwo przestało być domeną wyłącznie ekspertów ICT – to dziś kwestia strategiczna, decydująca o suwerenności państwa, jego stabilności gospodarczej i bezpieczeństwie obywateli. Polska, jeśli chce odgrywać rolę regionalnego lidera, musi potraktować ten obszar priorytetowo.

> ***Cyberbezpieczeństwo przestało być domeną wyłącznie ekspertów ICT – to dziś kwestia strategiczna, decydująca o suwerenności państwa, jego stabilności gospodarczej i bezpieczeństwie obywateli.***

Zależność technologiczna a bezpieczeństwo państwa

Jednym z kluczowych kierunków wzmacniania cyberbezpieczeństwa jest rozwój krajowego sektora ICT – to nie tylko szansa na przyspieszenie wzrostu gospodarczego, ale przede wszystkim warunek konieczny dla zachowania pełnej suwerenności. Historia Edwarda Snowdena, uświadomiła nam skalę inwigilacji prowadzonej przez NSA, przypadki wykorzystywania przez Stany Zjednoczone luk w zagranicznym oprogramowaniu czy szpiegowania europejskich polityków. Nawet bliscy sojusznicy nie wahają się używać narzędzi wywiadowczych wobec partnerów. Polska musi zatem rozwijać własne zdolności rozpoznawcze – zarówno techniczne, jak i analityczne – i uniezależniać się od infrastruktury znajdującej się pod jurysdykcją obcych państw. W tym kontekście należy podkreślić, jak bardzo niepokojącym precedensem było wykorzystywanie narzędzi takich jak izraelski Pegasus do inwigilacji nie tylko przestępców, ale też polskich dziennikarzy i polityków. We współczesnej cyberprzestrzeni zasada „*trust no one*" powinna być żelazną regułą.

Z tego względu Polska powinna wprowadzić niezależną kontrolę nad zakupami technologicznymi, wspierać rozwój rodzimego oprogramowania i wzmacniać krajowe kompetencje w zakresie wykrywania oraz analizy złośliwego kodu. Szczególnie istotnym zagrożeniem jest brak kontroli nad komunikacją rządową. Jeśli zagraniczne służby mają dostęp do korespondencji polskich decydentów, mogą wpływać na kierunki polityki, szantażować lub manipulować. To realne ryzyko utraty suwerenności. Dlatego komunikacja władz publicznych powinna być realizowana z wykorzystaniem infrastruktury pozostającej pod nadzorem państwa, przy zastosowaniu bezpiecznych protokołów i rozwiązań kryptograficznych.

Krytyczna infrastruktura i kompetencje cyfrowe

Polska musi także pilnie nadrobić zaległości w zakresie budowy zintegrowanego systemu łączności PPDR (*Public Protection and Disaster Relief*) – czyli infrastruktury komunikacyjnej dla służb ratunkowych i mundurowych. Brak takiego ogólnokrajowego, odpornego na zakłócenia i niezależnego systemu dla policji, straży pożarnej, pogotowia czy wojska to poważna luka w architekturze bezpieczeństwa narodowego. Polska – jako jeden z ostatnich krajów Unii Europejskiej – wciąż nie wdrożyła nowoczesnego i spójnego rozwiązania w tym obszarze.

Jeśli na poważnie myślimy o suwerenności cyfrowej, to musimy opierać się na regule „trust no one". Rozwijać własne kompetencje, rodzime zdolności produkcyjne i zachowywać kontrolę nad infrastrukturą. Bez krajowego sektora ICT i bezpiecznej komunikacji rządowej, państwo naraża się na zewnętrzny wpływ, inwigilację i utratę niezależności.

Tymczasem doświadczenia międzynarodowe pokazują, że wprowadzenie systemów PPDR w modelu partnerstwa publiczno-prywatnego może przynieść podwójną korzyść: wzmocnić bezpieczeństwo obywateli i napędzać rozwój gospodarki. Na wzór amerykańskiego

FirstNet czy brytyjskiego ESN, Polska mogłaby zbudować rdzeń sieci zapewniający bezpieczeństwo i niezawodność, podczas gdy operatorzy telekomunikacyjni – wyłonieni w drodze przetargu – odpowiadaliby za zapewnienie zasięgu i infrastrukturę dostępową. Takie rozwiązanie umożliwiałoby synergię sektora publicznego i prywatnego, obniżenie kosztów i podniesienie efektywności inwestycji.

Rozwój narodowego systemu PPDR mógłby stać się telekomunikacyjnym odpowiednikiem CPK – impulsem dla rodzimego sektora technologicznego. Otworzyłby przestrzeń dla budowy kompetencji, tworzenia miejsc pracy, rozwijania własności intelektualnej i modernizacji rozwiązań dla sektorów krytycznych. Mógłby pomóc przełamać wieloletni impas w zakresie wdrażania państwowych systemów takich jak LTE 450 dla energetyki czy GSM-R dla kolei. Przykłady Korei Południowej i innych państw pokazują, że zintegrowane wdrożenia systemów komunikacji krytycznej są nie tylko możliwe, ale i opłacalne – dla bezpieczeństwa państwa i jego gospodarki.

Trzeba pamiętać, że nawet najlepiej zabezpieczony system łączności i najnowocześniejszy sprzęt nie gwarantują bezpieczeństwa, jeśli zawodzi czynnik ludzki. Największych zagrożeń cybernetycznych należy upatrywać nie w obszarze komputerów i algorytmów, lecz w sferze oddziaływania czynników ludzkich – nieuwaga, złe nawyki i brak świadomości użytkowników to poważne zagrożenia dla całego systemu. Przykład afery mailowej z udziałem Michała Dworczyka pokazał, jak katastrofalne mogą być skutki skutecznego *phishingu* i zlekceważenia podstawowej cyberhigieny. W dzisiejszych realiach atakujący nie muszą bowiem przełamywać skomplikowanych zabezpieczeń – wystarczy słabe hasło, używane w wielu miejscach, brak uwierzytelnienia dwuskładnikowego lub kliknięcie w fałszywy link.

Brak zintegrowanego systemu łączności dla służb to luka w bezpieczeństwie, którą Polska musi pilnie zamknąć. Rozwój krajowego PPDR może nie tylko wzmocnić ochronę obywateli, ale stać się impulsem dla innowacji, gospodarki i odbudowy technologicznej suwerenności.

Konieczne wydaje się wprowadzenie obowiązkowych szkoleń z zakresu cyberbezpieczeństwa dla wszystkich pracowników sektora publicznego. Ich ukończenie powinno być traktowane jak swoiste „prawo jazdy" do poruszania się w cyberprzestrzeni. Należy również spopularyzować obowiązek korzystania z uwierzytelniania dwuskładnikowego, a także wdrożyć regularne audyty i testy odporności systemów informatycznych. Jak pokazują badania fundacji Digital Poland[1] na reprezentatywnej grupie Polaków, aż 45% z nas nabiera się na spersonalizowane kampanie *phishingowe* – to statystyka, która wymaga natychmiastowej reakcji instytucjonalnej i edukacyjnej.

1 Zob. https://digitalpoland.prowly.com/355483-65-polakow-martwi-sie-o-swoje-bezpieczenstwo-w-internecie--nowy-raport-fundacji-digital-poland-ujawnia-rosnace--zagrozenia-w-sieci [dostęp online].

Wymiar suwerenności cyfrowej ma również bezpośrednie przełożenie na kwestie obronności. Szacuje się, że już dziś około 25% wyposażenia wojskowego to komponenty cyfrowe – od systemów naprowadzania, przez oprogramowanie sterujące, po zintegrowane środowiska komunikacyjne. Doświadczenia z wojny w Ukrainie pokazują, że nieautoryzowany dostęp do takich systemów może prowadzić do ich zdalnej dezaktywacji lub do manipulacji parametrami działania uzbrojenia. Dlatego Polska musi posiadać krajowe zdolności w zakresie analizy kodów źródłowych, certyfikacji sprzętu i kontroli nad krytycznymi komponentami cyfrowymi w wojsku.

Największych zagrożeń cybernetycznych należy upatrywać nie w obszarze komputerów i algorytmów, lecz w obszarze oddziaływania czynników ludzkich – nieuwaga, złe nawyki i brak świadomości użytkowników to poważne zagrożenia dla całego systemu. Czasem wystarczy słabe hasło, brak uwierzytelnienia dwuskładnikowego lub kliknięcie w fałszywy link.

Warto tu przywołać przykład Izraela, który przy zakupie myśliwców F-35 Adir wynegocjował prawo do modyfikowania ich oprogramowania oraz pełnej kontroli nad pokładowymi systemami informatycznymi. Pokazuje to, że suwerenność cyfrowa jest możliwa nawet w relacjach z największymi partnerami zbrojeniowymi – o ile państwo potrafi jasno zdefiniować swoje potrzeby i wyegzekwować je w negocjacjach. Polska nie może pozostać pasywnym odbiorcą technologii, pozbawionym wpływu na ich działanie, jak ma to miejsce w niektórych państwach Zatoki Perskiej.

Aby tego uniknąć, potrzebne są inwestycje w rozwój rodzimego przemysłu obronnego i technologii podwójnego zastosowania – szczególnie w obszarach takich jak drony, sztuczna inteligencja i zaawansowana elektronika. Obszary te nie tylko zwiększają potencjał obronny, ale mogą także stać się katalizatorem rozwoju gospodarczego – o ile będą oparte na krajowym *know-how*, innowacjach *deep tech* oraz wynikach badań komercjalizowanych przez polskie uczelnie i instytuty badawcze.

Europejska droga do odporności cyfrowej

Wzmacnianie polskiej suwerenności cyfrowej powinno odbywać się nie tylko przez rozwój krajowych kompetencji i systemów, ale także poprzez aktywne uczestnictwo w tworzeniu europejskiej alternatywy wobec rozwiązań technologicznych spoza UE. Polska, wspólnie z innymi państwami członkowskimi, powinna rozwijać sektor ICT oparty na europejskich standardach i wartościach. Tym bardziej, że statystyki i analizy pokazują, jak wiele zagrożeń wiąże się z powszechnie używanym pozaeuropejskim sprzętem i oprogramowaniem – np. Fortinet czy Palo Alto[2] zawiera szereg krytycznych luk bezpieczeństwa. Andrew Grotto, były dyrektor ds. polityki cyberbezpieczeństwa w administracjach Obamy i Trumpa, otwarcie wskazywał na Microsoft jako potencjalne zagrożenie dla bezpieczeństwa narodowego

2 Zob. https://www.wnp.pl/tech/popularne-programy-mialy-chronic-firmy-okazaly-sie-furtkami-dla-hakerow-uzywa-ich-administracja,941032.html [dostęp online].

USA – ze względu na monopolistyczne rozprzestrzenienie systemów Windows i niedociągnięcia w polityce bezpieczeństwa[3].

Głośne incydenty – jak ubiegłoroczna awaria systemów CrowdStrike, która sparaliżowała miliony urządzeń – przypominają, jak ryzykowne jest uzależnienie od zamkniętych, scentralizowanych rozwiązań. Polska powinna stopniowo odchodzić od takich ekosystemów, promować *open source*, wspierać rozwój krajowych i europejskich rozwiązań oraz dywersyfikować współpracę technologiczną, szczególnie w odniesieniu do firm podlegających przepisom spoza UE.

Zagrożenie dotyczy nie tylko infrastruktury – również danych. Amerykańskie przepisy, takie jak Cloud Act[4] czy słynna sekcja FISA 702[5], umożliwiają służbom USA dostęp do danych przechowywanych w chmurze, niezależnie od ich fizycznego położenia. Oznacza to realne zagrożenie dla polskich instytucji publicznych korzystających z popularnych usług chmurowych. Dlatego Polska powinna rozwijać bezpieczną chmurę rządową oraz wspierać tworzenie europejskiej infrastruktury, np. w ramach takich inicjatyw jak Gaia-X[6]. Nowe rozporządzenie Data Act, które wejdzie w życie 12 września, może posłużyć jako narzędzie do wymuszania zgodności z europejskimi standardami w przetargach publicznych.

Równolegle konieczna jest harmonizacja krajowych regulacji z prawem unijnym. Implementacja dyrektywy NIS2, dotyczącej minimalnych standardów cyberbezpieczeństwa, stanowi szansę na stworzenie spójnych zasad obowiązujących we wszystkich państwach wspólnoty. Nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa powinna być nie tylko zgodna z unijnymi wymogami, lecz także analogiczna do przepisów stosowanych przez inne kraje. Dzięki temu polskie firmy zyskają łatwiejszy dostęp do innych rynków UE, uproszczone procedury certyfikacyjne oraz większą konkurencyjność. Zharmonizowane i transparentne przepisy ograniczą ryzyko korupcji i zapewnią większą przewidywalność w procesach decyzyjnych. To jest szczególnie istotne w kontekście obserwowanych na świecie przypadków odejścia niektórych państw od skutecznych regulacji antykorupcyjnych.

Suwerenność cyfrowa Polski wymaga nie tylko rozwoju krajowych kompetencji, lecz także aktywnego udziału w procesie tworzenia europejskiej alternatywy technologicznej. Tylko silne, odporne i niezależne cyfrowo państwo może skutecznie chronić swoje dane, instytucje i społeczeństwo przed presją zewnętrzną i informacyjną manipulacją.

W dyskusji o cyberbezpieczeństwie nie można pominąć aspektu wojny hybrydowej. Współczesna cyberprzestrzeń to nie tylko sieci i dane, lecz także pole walki informacyjnej. Dezinformacja, kampanie wpływu i manipulacja w mediach społecznościowych mogą realnie

3 Zob. https://www.inc.com/kit-eaton/why-a-former-white-house-cyber-director-called-microsoft-a-national-security-risk.html [dostęp online].
4 Zob. https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/ [dostęp online].
5 Zob. https://www.euronews.com/next/2024/06/01/heres-what-a-us-surveillance-law-means-for-european-data-privacy [dostęp online].
6 Zob. https://gaia-x.eu/ [dostęp online].

wpływać na decyzje polityczne i społeczne. Przykład referendum brexitowego pokazuje, że fałszywe treści mogą kształtować bieg historii. Polska – znajdująca się na styku interesów geopolitycznych i będąca celem licznych operacji informacyjnych – musi budować społeczną odporność na tego rodzaju działania. Wymaga to przemyślanej strategii komunikacji kryzysowej, wsparcia dla niezależnych organizacji *fact-checkingowych* oraz realnych regulacji dla cyfrowych platform – w zakresie zarówno szybkiego usuwania fałszywych treści jak i przejrzystości moderacji czy przeciwdziałania manipulacjom.

Równolegle należy prowadzić długofalowe programy edukacyjne w zakresie rozpoznawania manipulacji, krytycznej analizy treści medialnych oraz budowy kompetencji informacyjnych – zwłaszcza wśród młodzieży. Tylko społeczeństwo świadome, odporne i kompetentne informacyjnie może skutecznie przeciwstawić się narzędziom wojny kognitywnej. ■

O AUTORZE

Piotr Mieczkowski – Członek zarządu KIGEIT oraz Wiceprezes European AI Forum zrzeszającej ponad 2200 startupów AI z Europy. Posiada blisko 20-letnie doświadczenie zdobyte w sektorze TMT, obejmujące transformację cyfrową, tworzenie programów krajowych wspierających innowacyjność, wdrażanie strategii biznesowych, analizę rynków i usług, a także opracowywanie polityk publicznych w sektorze nowych technologii.